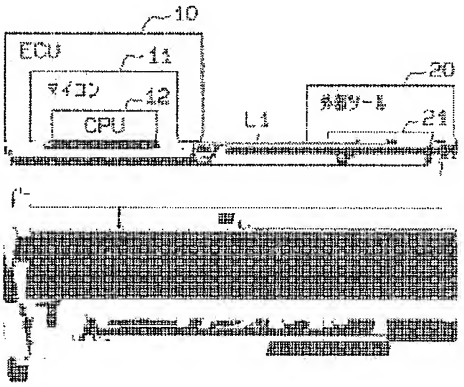
METHOD FOR INSPECTING ON-VEHICLE CONTROL UNIT

Publication number: JP2001202266 (A)
Publication date: 2001-07-27
Inventor(s): NAKAYAMA KIYONARI; KAMIYA KENJI; AOKI CHIZURU +
Applicant(s): DENSO CORP +
Classification:
- international: ***G06F11/22; G06F11/00;*** **G06F11/22; G06F11/00;** (IPC1-7): G06F11/22; G06F11/00
- European:
Application number: JP20000012803 20000121
Priority number(s): JP20000012803 20000121

Abstract of **JP 2001202266 (A)**

PROBLEM TO BE SOLVED: To rightly inspect an on-vehicle control unit and to prevent illegal alteration as the result. SOLUTION: An ECU 10 is provided with a widely known microcomputer 11, which is provided with a CPU 12 forming the center of various kinds of control, a flash memory 13 which can be erased and written electrically, and the other input/output circuit, etc., not shown in the figure. An external tool 20 is also provided with a widely known microcomputer 11 consisting of a CPU, a memory, an input/output circuit, etc. On judging (inspecting) the authenticity of the ECU 10, the tool 20 first transmits transmission data including a sum value calculation command and a random number to the ECU 10. The ECU 10 calculates the sum value of data in the memory 13 and enciphers the sum value in accordance with the random number by using a prescribed enciphering algorithm. After then, the enciphered sum value is transmitted to the tool 20, which compares and judges a decoded sum value and a previously registered true sum value to judge whether the ECU 10 is normal or abnormal by the result of it.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－202266
（P2001－202266A）
(43)公開日　平成13年７月27日(2001.7.27)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	11/22	３４０	Ｇ０６Ｆ 11/22	３４０Ｂ	５Ｂ０４８
		３１０		３１０Ｆ	
	11/00	３４０	11/00	３４０	

審査請求　未請求　請求項の数６　ＯＬ　（全 12 頁）

(21)出願番号　特願2000－12803(P2000－12803)

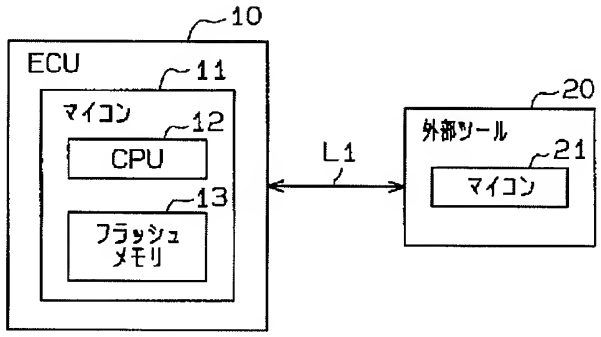
(22)出願日　平成12年１月21日(2000.1.21)

(71)出願人　000004260
株式会社デンソー
愛知県刈谷市昭和町１丁目１番地
(72)発明者　中山　聖也
愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内
(72)発明者　神谷　健治
愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内
(74)代理人　100068755
弁理士　恩田　博宣　（外１名）

最終頁に続く

(54)【発明の名称】　車載制御ユニットの検査方法

(57)【要約】
【課題】車載制御ユニットを正しく検査し、ひいては不正改造の防止を図る。
【解決手段】ＥＣＵ１０は周知のマイコン１１を備え、マイコン１１は、各種制御の中枢をなすＣＰＵ１２、電気的に消去及び書き込み可能なフラッシュメモリ１３、その他図示しない入出力回路等を備える。外部ツール２０も同様に、ＣＰＵ、メモリ、入出力回路等からなる周知のマイコン２１を備える。ＥＣＵ１０の正偽判定（検査）に際し、外部ツール２０では先ず、サム値算出指令と乱数とを含む送信データをＥＣＵ１０に送信する。ＥＣＵ１０では、フラッシュメモリ１３内のデータのサム値を算出すると共に、所定の暗号化アルゴリズムを用い、乱数に応じてサム値を暗号化する。その後、暗号化サム値を外部ツール２０に送信する。外部ツール２０では、復号化したサム値と予め登録されている真のサム値とを比較判定し、その結果によりＥＣＵ１０が正常か異常かを判断する。



1

【特許請求の範囲】

【請求項１】車載制御ユニット内のメモリについてデータのサム値を求め、該サム値により本制御ユニットを検査する車載制御ユニットの検査方法において、

乱数を発生させ、その乱数をサム値の算出指令と共に外部ツールから制御ユニットへ送信する第１のステップと、

前記メモリのサム値を算出すると共に、該サム値を前記乱数に応じて暗号化する第２のステップと、

前記暗号化したデータを外部ツールに送信する第３のステップと、

外部ツールで受信したデータを復号化すると共に、そのデータ中のサム値を予め用意された真のサム値と比較し、その比較判定の結果から車載制御ユニットを検査する第４のステップと、からなることを特徴とする車載制御ユニットの検査方法。

【請求項２】車載制御ユニット内のメモリは、電気的に書き換え可能な不揮発性メモリである請求項１に記載の車載制御ユニットの検査方法。

【請求項３】前記第４のステップにおいてサム値が不一致となった場合、前記第１のステップに戻って新たに乱数を設定し、それに続く第２～第４のステップを再度実施する請求項１又は２に記載の車載制御ユニットの検査方法。

【請求項４】複数の暗号化アルゴリズムを車載制御ユニットに予め用意しておき、

前記第１のステップでは、複数の暗号化アルゴリズムの中から一つを指定してそれを表す識別データを、乱数とサム値の算出指令と共に外部ツールから制御ユニットへ送信し、

前記第２のステップでは、前記識別データによる指定通りの暗号化アルゴリズムを使って暗号化を行い、

その後、前記第４のステップでは、前記指定した暗号化アルゴリズムに対応する復号化の算出式を取り出して受信データを復号化し、サム値を抽出する請求項１又は２に記載の車載制御ユニットの検査方法。

【請求項５】車載制御ユニットは、電気的に書き換え可能な不揮発性メモリを実装した第１マイクロコンピュータと、書き換え不可能なＲＯＭを実装した第２マイクロコンピュータとを備え、第２マイクロコンピュータのＲＯＭに、前記不揮発性メモリのサム値を暗号化するための暗号化アルゴリズムを記憶させておく請求項１～４の何れかに記載の車載制御ユニットの検査方法。

【請求項６】請求項５に記載の車載制御ユニットの検査方法において、

前記第２のステップは、前記不揮発性メモリのサム値を第１マイクロコンピュータから第２マイクロコンピュータへ送信するステップと、第２マイクロコンピュータにて前記ＲＯＭ内の暗号化アルゴリズムでサム値を暗号化した後、その暗号化データを第１マイクロコンピュータに返信するステップと、を含むものである車載制御ユニットの検査方法。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、車載制御ユニットの検査方法に関するものである。

【０００２】

【従来の技術】この種の従来技術として、特開平１１－１３２０９７号公報の「車両制御用メモリ書き換え装置」がある。同公報の装置は、外部ツールにより電気的に消去及び書き込み可能な制御メモリ（フラッシュメモリ）を搭載したＥＣＵ（車載制御ユニット）を備え、書き換え許可された時にのみ前記制御メモリに対するデータ書き換えが実施される。また、この装置は、制御メモリが記憶するソフトウエア（制御プログラム）が正しいことを検査するものであり、その特徴として、

・予め記憶しておいた制御メモリのサム値（真値）と、ＥＣＵで算出したサム値とを共に表示し、それらを比較することで正偽判定を行う。

・上記サム値の比較は外部ツールの内部で行い、その結果（正偽）のみを返信する。

・イグニッションキースイッチのＯＦＦからＯＮへの切換後にサム値の計算を行う。といった処理を実行する。

【０００３】

【発明が解決しようとする課題】上記公報の従来技術では、ＥＣＵで計算したサム値を外部ツールに対してそのまま送信する。そのため、ＥＣＵと外部ツールとの通信データをモニタすることにより、ＥＣＵにより算出した正しいサム値を容易に知り得ることができる。

【０００４】また、制御メモリのサム値は、ソフトウエアを書き換えなければ変化しないものであるため、外部チェッカに対して正しいサム値を常に送信するような不正なプログラムを不正改造者が作成し、それをＥＣＵに組み込めば、正規のサム値算出アルゴリズムを知らなくても容易に正規ＥＣＵとしてなりすますことが可能となる。これは、ＥＣＵ側で正偽判定を行う構成でも同様である。すなわち、モニタしたサム値を返答する偽プログラムを不正改造者が作成することにより、不正改造された偽ＥＣＵであっても、外部ツールは正しいサム値（常に同じ）が返答されたと認識し、正しいＥＣＵであると判断してしまう。

【０００５】本発明は、上記問題に着目してなされたものであって、その目的とするところは、車載制御ユニットを正しく検査し、ひいては不正改造の防止を図ることができる車載制御ユニットの検査方法を提供することである。

【０００６】

【課題を解決するための手段】請求項１に記載の車載制御ユニットの検査方法では、（１）乱数を発生させ、その乱数をサム値の算出指令と共に外部ツールから制御ユ

ニットへ送信する第１のステップ、（２）前記メモリのサム値を算出すると共に、該サム値を前記乱数に応じて暗号化する第２のステップ、（３）前記暗号化したデータを外部ツールに送信する第３のステップ、（４）外部ツールで受信したデータを復号化すると共に、そのデータ中のサム値を予め用意された真のサム値と比較し、その比較判定の結果から車載制御ユニットを検査する第４のステップ、といった各ステップを順に実施するので、不正改造を行おうとする者に正しいサム値が漏れ知れる可能性は低くなる。また、仮に正規の制御ユニットが不正改造され、メモリの正しいサム値を外部ツール側に返信できるような不正なプログラムが制御ユニットに組み込まれたとしても、外部ツールでは、暗号化データを受信すると共にその暗号化データを復号化した後、サム値の比較判定を行うので、不正改造された制御ユニットが正規な制御ユニットとしてなりすますことが極めて困難になる。その結果、車載制御ユニットを正しく検査し、ひいては不正改造の防止を図ることができる。

【０００７】上記発明は特に、フラッシュメモリ等、電気的に書き換え可能な不揮発性メモリにて車載制御ユニット内のメモリが構成される場合に有効である（請求項２）。

【０００８】請求項３に記載の発明では、前記第４のステップにおいてサム値が不一致となった場合、前記第１のステップに戻って新たに乱数を設定し、それに続く第２～第４のステップを再度実施する。これにより、一時的な通信異常が原因で正しく検査されなかった場合にも、再通信により適正な検査が実施できる。またここで、乱数を再設定するために制御ユニットと外部ツールとの間の送受信データはその都度異なるので、通信線がモニタされることを想定しても、正しいサム値が漏れ知れる可能性は極めて低くなる。

【０００９】請求項４に記載の発明では、

・前記第１のステップでは、複数の暗号化アルゴリズムの中から一つを指定してそれを表す識別データを、乱数とサム値の算出指令と共に外部ツールから制御ユニットへ送信し、

・前記第２のステップでは、前記識別データによる指定通りの暗号化アルゴリズムを使って暗号化を行い、

・その後、前記第４のステップでは、前記指定した暗号化アルゴリズムに対応する復号化の算出式を取り出して受信データを復号化し、サム値を抽出する。

【００１０】かかる場合、複数の暗号化アルゴリズムを択一的に使うことにより、不正改造者に暗号化アルゴリズムが知られたとしても、実際に使われた暗号化アルゴリズムに対応させてサム値を解明するのは非常に困難となる。それ故、車載制御ユニットの不正改造を、より一層困難なものとすることができる。

【００１１】請求項５に記載の発明では、車載制御ユニットは、電気的に書き換え可能な不揮発性メモリを実装

した第１マイクロコンピュータと、書き換え不可能なＲＯＭを実装した第２マイクロコンピュータとを備え、第２マイクロコンピュータのＲＯＭに、前記不揮発性メモリのサム値を暗号化するための暗号化アルゴリズムを記憶させておく。つまり、書き換え不可能な第２マイクロコンピュータのＲＯＭにサム値の暗号化アルゴリズムを配置することにより、不正改造防止が更に強化される。

【００１２】かかる請求項５の発明では、請求項６に記載したように、第２のステップを実現する上で、前記不揮発性メモリのサム値を第１マイクロコンピュータから第２マイクロコンピュータへ送信するステップと、第２マイクロコンピュータにて前記ＲＯＭ内の暗号化アルゴリズムでサム値を暗号化した後、その暗号化データを第１マイクロコンピュータに返信するステップと、を設けると良い。

【００１３】

【発明の実施の形態】（第１の実施の形態）この発明を具体化した本実施の形態では、エンジン制御等を司るＥＣＵにて車載制御ユニットを構成しており、このＥＣＵに対して外部ツールを接続し、当該ＥＣＵの検査やデータの交換等を行うこととしている。以下、その詳細を図面に従って説明する。

【００１４】図１は、制御システムの概略構成を示すブロック図である。本システムにおいて、ＥＣＵ１０は周知のマイクロコンピュータ（以下、マイコンという）１１を備え、マイコン１１は、予め用意されている制御プログラム等を用いてエンジンの各種制御を実施する。マイコン１１は、各種制御の中枢をなすＣＰＵ１２、電気的に消去及び書き込み可能なフラッシュメモリ１３、その他図示しないＲＡＭや入出力回路等を備える。

【００１５】外部ツール２０も同様に、ＣＰＵ、メモリ、入出力回路等からなる周知のマイコン２１を備える。この外部ツール２０は、ＥＣＵ１０の正偽判定等の検査や、同ＥＣＵ１０内のフラッシュメモリ１３のデータ書き換えに際し、通信線Ｌ１を介してＥＣＵ１０に接続される。これにより、ＥＣＵ１０と外部ツール２０との間でシリアル通信によるデータのやり取りが行われる。

【００１６】ＥＣＵ１０の正偽判定（検査）の概要を、図２を用いて説明する。かかる場合、フラッシュメモリ１３内のデータのサム値と既知の正しいサム値とが比較され、両者が一致すれば、ＥＣＵ１０が正規なものであると判断される。このとき、外部ツール２０側では乱数を発生させてそれをＥＣＵ１０に送信する一方、ＥＣＵ１０側では、その内部に予め記憶された暗号化アルゴリズムを用い、サム値を暗号化して外部ツール２０に送信するようになっている。なお図２では、処理順序を表すため、（１）～（６）の連続番号を付している。

【００１７】先ず始めに、サム値の算出指令と乱数Ｒｔとを含む送信データを通信線Ｌ１を介して外部ツール２

０からＥＣＵ１０に送信する（図の（１））。このとき、外部ツール２０の送信データは、例えば図５（ａ）のフレーム構成を有し、このうち、送信ヘッダは送信元ＩＤ、送信先ＩＤ及びコマンドコードにて構成され、データは送信データＩＤ、乱数、本送信データのチェックサム（ＣＳ）にて構成されている。

【００１８】ＥＣＵ１０側では、フラッシュメモリ１３内のデータのサム値Ｘｓｕｍを算出すると共に、所定の暗号化アルゴリズムを用い、乱数Ｒｔに応じてサム値Ｘｓｕｍを暗号化する（図の（２），（３））。つまり、算出式Ｘｔ＝ｆ（Ｘｓｕｍ，Ｒｔ）により、暗号化したサム値Ｘｔ（以下には便宜上、暗号化サム値Ｘｔと言う）を算出する。

【００１９】その後、暗号化サム値Ｘｔを通信線Ｌ１を介して外部ツール２０に送信する（図の（４））。このとき、外部ツール２０の受信データは、例えば図５（ｂ）のフレーム構成を有し、このうち、送信ヘッダは送信元ＩＤ、送信先ＩＤ及びコマンドコードにて構成され、データは送信データＩＤ、暗号化データ、本送信データのチェックサム（ＣＳ）にて構成されている。

【００２０】外部ツール２０では、算出式

Ｘｓｕｍ＝ｆ-1（Ｘｔ，Ｒｔ）

により、暗号化サム値Ｘｔを復号化し、サム値Ｘｓｕｍを算出する（図の（５））。その後、前記の如く算出したサム値Ｘｓｕｍと、予め登録されている真のサム値Ｘｒｅｆとを比較判定する（図の（６））。そして、両者が一致すれば、ＥＣＵ１０が正規ＥＣＵであると判断し、不一致であれば、ＥＣＵ１０が偽ＥＣＵであると判断する。

【００２１】以下には、外部ツール２０によるＥＣＵ１０の正偽判定に際し、ＥＣＵ１０及び外部ツール２０内の各マイコン１１，２１により実施される処理の流れを図３及び図４のフローチャートに従い説明する。始めに、外部ツール２０の処理の流れを図３のフローチャートで説明する。

【００２２】例えば修理工場等において作業者が外部ツール２０を操作することで図３の処理がスタートし、先ずステップ１０１では、乱数発生処理を実行して乱数Ｒｔを設定し、続くステップ１０２では、コマンド送信を実施する。すなわち、乱数Ｒｔをサム値算出指令と共にＥＣＵ１０に送信する。また、ステップ１０３ではタイマセットを行う。このステップ１０１～１０３が通信前処理に相当する。

【００２３】その後、この外部ツール２０では、コマンド受信に対するＥＣＵ１０からの受信確認を行う。すなわち、タイムアウトしていないことを条件に（ステップ１０４がＮＯ）、ステップ１０５では、前記ステップ１０２のコマンド送信に対する応答をＥＣＵ１０から受信したか否かを判別する。応答が無いままタイムアウトした場合（ステップ１０４がＹＥＳ）、ステップ１０２に戻り、再度同じ乱数を用いてコマンド送信を実施する。そして、タイマセット、受信確認の各処理を再び実施する。

【００２４】なお、コマンド再送信の回数を予め制限しておき、例えばタイムアウトが３回繰り返されると、通信異常であると判断し、その旨のコードを記憶すると共に以降の処理を中止しても良い。また、１回でもタイムアウトになると、その時点で通信異常と判断しても良い。

【００２５】コマンド送信に対する応答を受信すると、ステップ１０６に進み、以降の受信後処理を実施する。すなわち、ステップ１０６では、ＥＣＵ１０から受信した暗号化サム値Ｘｔを復号化し、サム値Ｘｓｕｍの生データを抽出する。また、続くステップ１０７では、予め登録されている真のサム値Ｘｒｅｆを取り出す。

【００２６】その後、ステップ１０８では、サム値Ｘｓｕｍ（生データ）と真のサム値Ｘｒｅｆとを比較し、両サム値が一致すると判別されれば（ステップ１０９がＹＥＳ）、ＥＣＵ正常である旨を判断する。

【００２７】また、両サム値が不一致であれば（ステップ１０９がＮＯ）、ステップ１１０で予め定めた規定回数だけ通信を繰り返したか否かを判別する。ＮＯであればステップ１０１に戻る。これにより、別の乱数が再設定され、上述した処理が繰り返し実施される。そして、乱数の再設定及びそれに付随するサム値判定の処理が規定回数（例えば３回）だけ繰り返されてもサム値不一致のままであれば、ステップ１１０がＹＥＳとなり、ＥＣＵ異常である旨を判断する。

【００２８】次に、ＥＣＵ１０の処理の流れを図４のフローチャートに従い説明する。先ずステップ２０１では、外部ツール２０よりコマンドを受信したか否かを判別し、ＹＥＳであればステップ２０２に進み、受信データから乱数Ｒｔを抽出する。

【００２９】その後、ステップ２０３では、算出式

Ｘｓｕｍ＝ΣＤａｔａ（ｉ）

により、サム値Ｘｓｕｍを算出する。すなわち、フラッシュメモリ１３内の規定されたアドレス領域についてアドレスｉのデータを全て加算し、その和をサム値Ｘｓｕｍとする。

【００３０】その後、ステップ２０４では、前記受信した乱数Ｒｔでサム値Ｘｓｕｍを暗号化して暗号化サム値Ｘｔを求め、続くステップ２０５では、暗号化サム値Ｘｔを外部ツール２０に送信する。このデータ送信により、外部ツール２０では、前記図３のステップ１０５でデータ受信が確認されることとなる。

【００３１】なお本実施の形態では、図３のステップ１０１，１０２の処理が本発明の「第１のステップ」に、図４のステップ２０３，２０４の処理が「第２のステップ」に、図４のステップ２０５の処理が「第３のステップ」に、図３のステップ１０６～１０９の処理が「第４

のステップ」に、それぞれ該当する。

【００３２】以上詳述した本実施の形態によれば、以下に示す効果が得られる。つまり、上記ＥＣＵ１０の検査方法によれば、不正改造を行おうとする者に正しいサム値（算出したサム値Ｘｓｕｍ）が漏れ知れる可能性は低くなる。また、仮に正規のＥＣＵ１０が不正改造され、フラッシュメモリ１３の正しいサム値を外部ツール２０側に返信できるような不正なプログラムが偽ＥＣＵに組み込まれたとしても、外部ツール２０では、暗号化データを受信すると共にその暗号化データを復号化した後、サム値の比較判定を行うので、不正改造されたＥＣＵが正規なＥＣＵとしてなりすますことが極めて困難になる。その結果、ＥＣＵ１０を正しく検査し、ひいては不正改造の防止を図ることができる。

【００３３】また、サム値不一致の場合、新たに乱数Ｒｔを設定して再検査を行うので、一時的な通信異常が原因で正しく検査されなかった場合にも、再通信により適正な検査が実施できる。またここで、乱数Ｒｔを再設定するためにＥＣＵ１０と外部ツール２０との間の送受信データはその都度異なるので、通信線Ｌ１がモニタされることを想定しても、正しいサム値が漏れ知れる可能性は極めて低くなる。

【００３４】（第２の実施の形態）次に、本発明における第２の実施の形態を説明する。但し、本実施の形態では、上述した第１の実施の形態と同等であるものは説明を簡略化し、第１の実施の形態との相違点を中心に説明する。

【００３５】上記第１の実施の形態では不正改造が容認される可能性は極めて低いものの、万が一、暗号化アルゴリズムが不正改造者に漏れ知れた場合、不正改造が可能となる。その対策として、本実施の形態では、複数の暗号化アルゴリズム（算出式）を用意し、そのうちどのアルゴリズムを使用するかを外部ツール２０から指示する方法を提案する。なお本実施の形態では、制御システムとして前記図１の構成をそのまま流用する。

【００３６】本実施の形態におけるＥＣＵ１０の正偽判定（検査）の概要を、図６を用いて説明する。なお図６では、処理順序を表すため、（１）～（８）の連続番号を付している。

【００３７】先ず始めに、サム値の算出指令と、乱数Ｒｔと、暗号化アルゴリズムの識別コードＩＤとを含む送信データを通信線Ｌ１を介して外部ツール２０からＥＣＵ１０に送信する（図の（１））。このとき、外部ツール２０の送信データは、例えば前記図５（ａ）のフレーム構成に対し、データとして暗号化アルゴリズムの識別コードＩＤを追加した構成となる。

【００３８】ＥＣＵ１０側では、フラッシュメモリ１３内のデータのサム値Ｘｓｕｍを算出すると共に、外部ツール２０からの送信データに含まれる暗号化アルゴリズムの識別コードＩＤに基づき、それに相応する暗号化の

算出式を取り出す（図の（２），（３））。また、この算出式を用い、乱数Ｒｔに応じてサム値Ｘｓｕｍを暗号化する（図の（４））。つまり、算出式

Ｘｔ＝ｆ（Ｘｓｕｍ，Ｒｔ）

により、暗号化サム値Ｘｔを算出する。ここで、図示の如く、暗号化ＩＤが０ｘ０１，０ｘ０２，・・・０ｘＦのように与えられる場合、それに対応する算出式はｆ（＊，＊），ｇ（＊，＊），・・・ｔ（＊，＊）となり、これら何れかの算出式を用いてサム値Ｘｓｕｍが暗号化される。その後、暗号化サム値Ｘｔを通信線Ｌ１を介して外部ツール２０に送信する（図の（５））。

【００３９】外部ツール２０では、その時の暗号化アルゴリズムの識別コードＩＤに相応する復号化の算出式を取り出し、その算出式にて暗号化サム値Ｘｔを復号化する（図の（６），（７））。つまり、算出式

Ｘｓｕｍ＝ｆ-1（Ｘｔ，Ｒｔ）

により、サム値Ｘｓｕｍを算出する。

【００４０】その後、前記の如く算出したサム値Ｘｓｕｍと、予め登録されている真のサム値Ｘｒｅｆとを比較判定する（図の（８））。そして、両者が一致すれば、ＥＣＵ１０が正規ＥＣＵであると判断し、不一致であれば、ＥＣＵ１０が偽ＥＣＵであると判断する。

【００４１】以下には、外部ツール２０によるＥＣＵ１０の正偽判定に際し、ＥＣＵ１０及び外部ツール２０内の各マイコン１１，２１により実施される処理の流れを図７及び図８のフローチャートに従い説明する。

【００４２】始めに、外部ツール２０の処理の流れを図７のフローチャートで説明する。但し、図７は前記図３の一部のみを変更したものであり、実際には前記図３そのものに対し、ステップ３０１，３０２の処理を追加したことのみが相違する。以下、前記図３との相違点を中心に説明する。

【００４３】図７において、乱数発生処理の後、ステップ３０１では、多数の暗号化アルゴリズムの中から一つを選択する。そして、続くステップ１０２では、その暗号化アルゴリズムの識別コードＩＤを、乱数Ｒｔ及びサム値算出指令と共にＥＣＵ１０へ送信する。

【００４４】その後、ＥＣＵ１０からの受信確認を終えると、ステップ３０２では、暗号化アルゴリズムの識別コードＩＤに対応する復号化の算出式を取り出す。そしてそれ以降、図３で前述した通り、暗号化サム値Ｘｔの復号化、真のサム値Ｘｒｅｆとの比較判定等を行い、ＥＣＵ１０の正偽判定を実施する。

【００４５】次に、ＥＣＵ１０の処理の流れを図８のフローチャートに従い説明する。この図８の処理は前記図４に置き換えて実施される。図８では、外部ツール２０からのコマンド受信の旨を判別すると、ステップ４０１からステップ４０２に進み、受信データから乱数Ｒｔと暗号化アルゴリズムの識別コードＩＤ（アルゴリズムＮｏ．）とを抽出する。

【００４６】その後、ステップ４０３では、フラッシュメモリ１３内の規定されたアドレス領域についてアドレスｉのデータを全て加算し、その和によりサム値Ｘｓｕｍを算出する。

【００４７】その後、ステップ４０４では、指定の暗号化アルゴリズムを取り出し、続くステップ４０５では、サム値Ｘｓｕｍを暗号化して暗号化サム値Ｘｔを求める。更にステップ４０６では、暗号化サム値Ｘｔを外部ツール２０に送信する。このデータ送信により、外部ツール２０では、前記図７のステップ１０５でデータ受信が確認されることとなる。

【００４８】なお本実施の形態では、上記第１の実施の形態との違いとして、図７のステップ３０１の処理が「第１のステップ」に含まれ、同ステップ３０２の処理が「第４のステップ」に含まれる。また、図８のステップ４０２～４０５の処理が「第２のステップ」に、同ステップ４０６の処理が「第３のステップ」に、それぞれ該当する。

【００４９】以上第２の実施の形態によれば、複数の暗号化アルゴリズムを択一的に使うことにより、不正改造を行おうとする者に暗号化アルゴリズムが知られたとしても、実際に使われた暗号化アルゴリズムに対応させてサム値を解明するのは非常に困難となる。それ故、ＥＣＵ１０の不正改造を、より一層困難なものとすることができる。またこの場合、各々の暗号化アルゴリズムが簡単なものであっても、不正改造者がそのアルゴリズムを認識し、不正改造者両を車検に通す等、不正行為を行おうとすることが困難になる。

【００５０】（第３の実施の形態）複雑な制御が要求されるＥＣＵには、高い演算負荷を分散させるために複数のマイコン（ＣＰＵ）を備えて構成されるものがある。例えば２個のマイコンを持つ２マイコンシステムのＥＣＵにおいては、前記のフラッシュメモリを搭載し、エンジンの主要制御を受け持つメイン側のマイコンと、制御プログラムを市場で書き換え不可能なＲＯＭを搭載し、主要制御以外の制御を受け持つサブ側のマイコンとで構成することがある。

【００５１】図９は、本実施の形態における制御システムの概要を示す構成図である。図９の構成では、前記図１の構成との違いとして、ＥＣＵ３０は、第１マイコン（第１マイクロコンピュータ）３１と第２マイコン（第２マイクロコンピュータ）３２とを備える。第１マイコン３１は、燃料噴射制御や点火時期制御等、エンジンの主要な制御を受け持つマイコンであり、ＣＰＵ３１ａとフラッシュメモリ３１ｂとを実装する。また、第２マイコン３２は、トランスミッション制御等を受け持つマイコンであり、ＣＰＵ３２ａと、プログラムを市場で書き換え不可能なＲＯＭ３２ｂとを実装する。

【００５２】こうした２マイコンシステムのＥＣＵ３０において、第２マイコン３２のＲＯＭ３２ｂ内には、第１マイコン３１の正偽判定を行うために用いる暗号化アルゴリズムが格納されている。

【００５３】図１０は、第１マイコン３１の処理と第２マイコン３２の処理とを個々に示すフローチャートである。先ずは、図１０（ａ）に従い、第１マイコン３１の処理の流れを説明する。

【００５４】図１０（ａ）では、外部ツール２０からのコマンド受信の旨を判別すると、ステップ５０１からステップ５０２に進み、受信データから乱数Ｒｔを抽出する。その後、ステップ５０３では、フラッシュメモリ３１ｂ内の規定されたアドレス領域についてアドレスｉのデータを全て加算し、その和によりサム値Ｘｓｕｍを算出する。その後、ステップ５０４では、前記受信した乱数Ｒｔと、前記算出したサム値Ｘｓｕｍとを第２マイコン３２に送信する。

【００５５】続くステップ５０５では、第２マイコン３２へのデータ送信に応答して当該第２マイコン３２からデータ受信をしたか否かを判別する。この受信データには、第２マイコン３２で暗号化された暗号化サム値Ｘｔが含まれており、データ受信を確認した後、ステップ５０６では、暗号化サム値Ｘｔを外部ツール２０に送信する。このデータ送信により、外部ツール２０では、前記図３のステップ１０５でデータ受信が確認されることとなる。

【００５６】次に、第２マイコン３２の処理の流れを図１０（ｂ）のフローチャートに従い説明する。図１０（ｂ）では、前記図１０（ａ）のステップ５０４におけるデータ送信を伴い、第１マイコン３１からのデータ受信の旨を判別すると、ステップ６０１からステップ６０２に進み、受信データから乱数Ｒｔとサム値Ｘｓｕｍとを抽出する。その後、ステップ６０３では、ＲＯＭ３２ｂ内に用意されている所定の暗号化アルゴリズムを用い、サム値Ｘｓｕｍを暗号化して暗号化サム値Ｘｔを求める。続くステップ６０４では、暗号化サム値Ｘｔを第１マイコン３１に送信する。このデータ送信により、第１マイコン３１では、前記図１０（ａ）のステップ５０５でデータ受信が確認されることとなる。そして更に、このデータが外部ツール２０に送信される。

【００５７】なお本実施の形態では、上記第１の実施の形態との違いとして、図１０（ａ）のステップ５０３，５０４及び図１０（ｂ）のステップ６０３の処理が「第２のステップ」に、図１０（ａ）のステップ５０６の処理が「第３のステップ」に、それぞれ該当する。

【００５８】以上第３の実施の形態によれば、第２マイコン３２のＲＯＭ３２ｂに暗号化アルゴリズムを記憶させておくので、暗号化アルゴリズムを不正に書き換えることが不可能となり、不正改造防止が更に強化される。

【００５９】上記第３の実施の形態では、第２マイコン３２のＲＯＭ３２ｂに所定の暗号化アルゴリズムを記憶させる構成であったが、この構成を変更しても良い。例

11

えば、既述した第２の実施の形態のように、第２マイコン３２のＲＯＭ３２ｂに複数の暗号化アルゴリズムを記憶させておき、外部ツール２０から指定される識別コードに従い、複数の暗号化アルゴリズムの中から一つを選択する構成としても良い。

【００６０】また、同じく第３の実施の形態では、外部ツール２０から送信される乱数Ｒｔを一旦第１マイコン３１で受信し、その後、サム値と共に第２マイコン３２へ転送したが、この乱数Ｒｔを外部ツール２０から第２マイコン３２へ直接送信する構成としても良い。

【図面の簡単な説明】

【図１】発明の実施の形態における制御システムの概略構成を示すブロック図。

【図２】ＥＣＵの正偽判定の様子を示す説明図。

【図３】外部ツールの処理の流れを示すフローチャート。

【図４】ＥＣＵの処理の流れを示すフローチャート。

12

【図５】送信データ及び受信データのフレーム構成を示す図。

【図６】第２の実施の形態においてＥＣＵの正偽判定の様子を示す説明図。

【図７】第２の実施の形態において外部ツールの処理の流れを示すフローチャート。

【図８】第２の実施の形態においてＥＣＵの処理の流れを示すフローチャート。

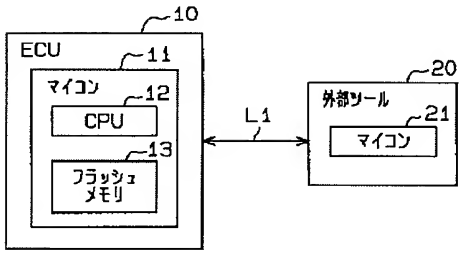
【図９】第３の実施の形態において制御システムの概略構成を示すブロック図。

【図１０】第３の実施の形態において第１マイコン及び第２マイコンの処理の流れを示すフローチャート。

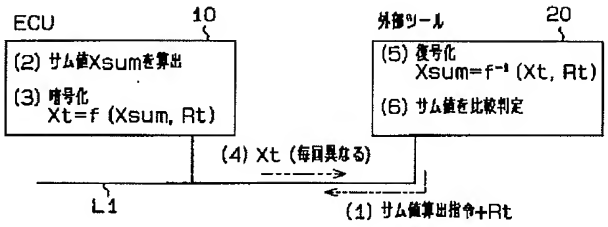
【符号の説明】

１０…ＥＣＵ、１１…マイコン、１２…ＣＰＵ、１３…フラッシュメモリ、２０…外部ツール、３０…ＥＣＵ、３１…第１マイコン、３１ｂ…フラッシュメモリ、３２…第２マイコン、３２ｂ…ＲＯＭ。

【図１】



【図２】



【図５】

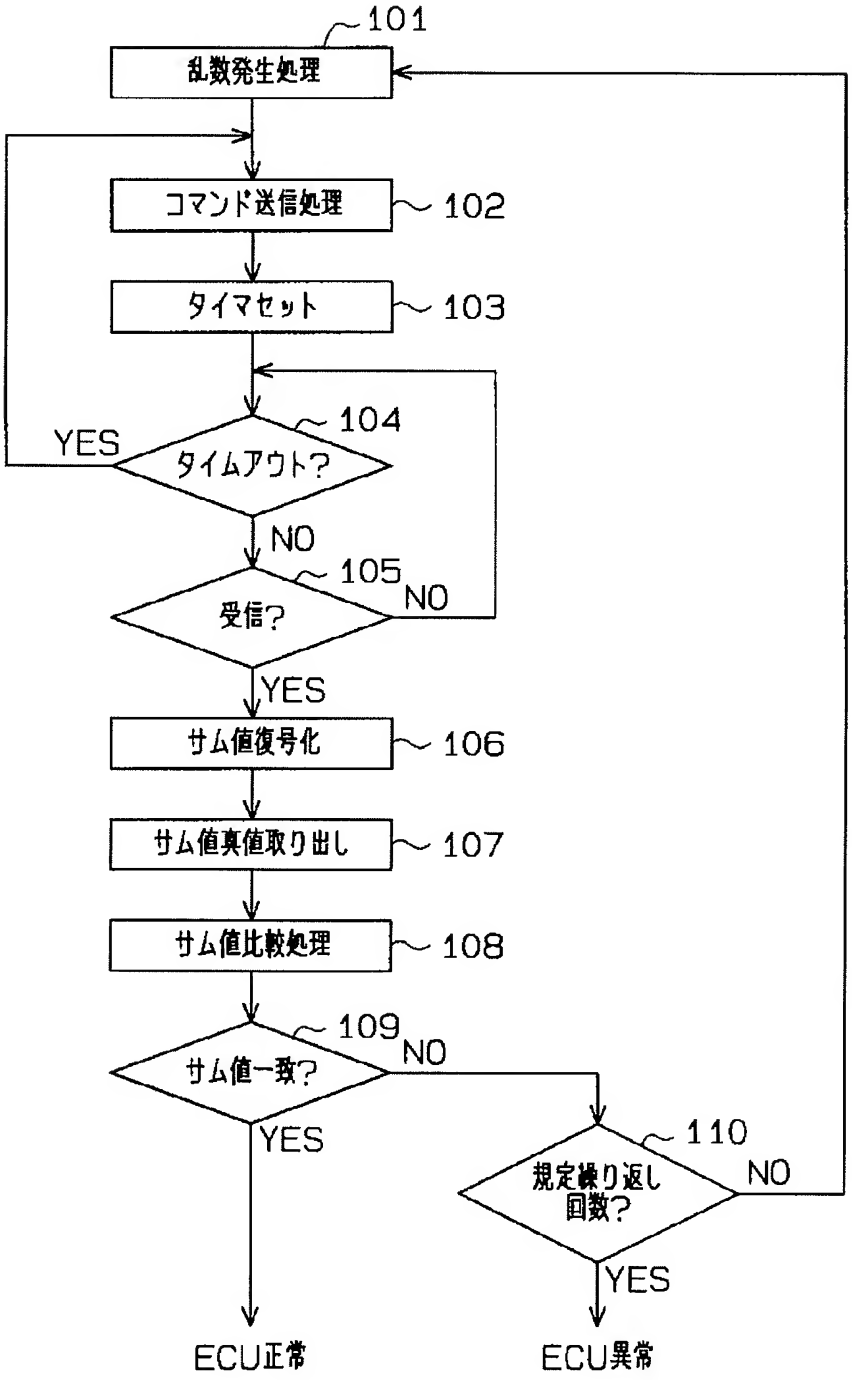
(a) 送信データの例

送信ヘッダ (送信元ID、送信先ID、コマンドコード)	データ (送信データID、乱数、CS)

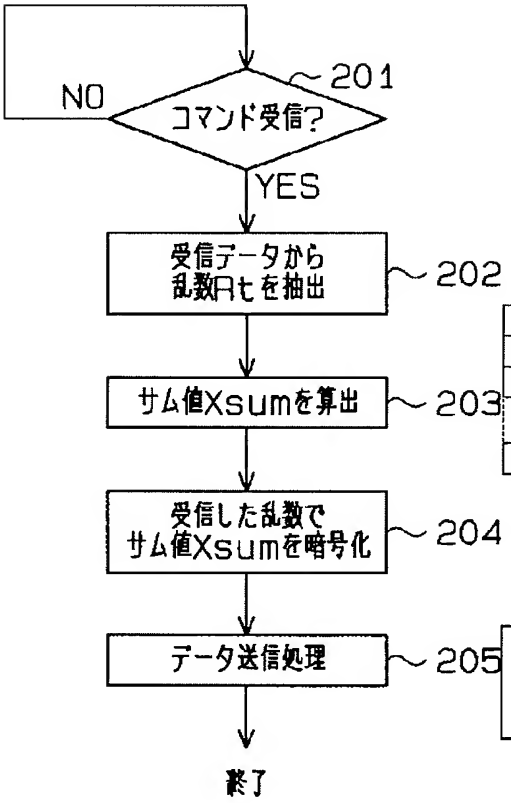
(b) 受信データの例

送信ヘッダ (送信元ID、送信先ID、コマンドコード)	データ (送信データID、暗号化データ、CS)

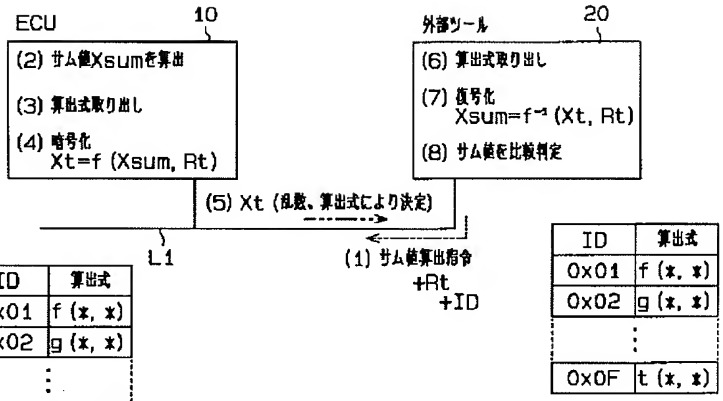
【図３】


101
乱数発生処理
コマンド送信処理
102
タイマセット
103
104
YES
タイムアウト?
NO
105
受信?
NO
YES
サム値復号化
106
サム値真値取り出し
107
サム値比較処理
108
109
サム値一致?
NO
YES
110
規定繰り返し回数?
NO
YES
ECU正常
ECU異常

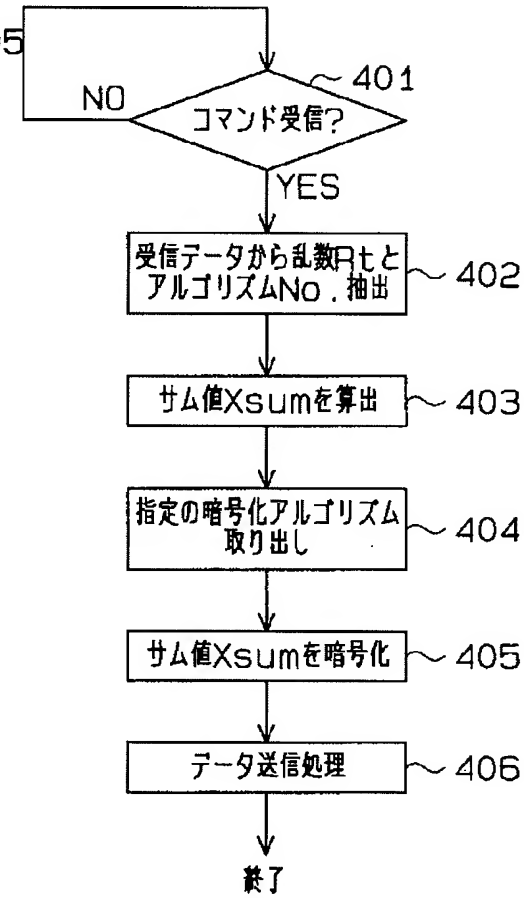
【図４】


NO
201
コマンド受信?
YES
受信データから
乱数Rtを抽出
202
サム値Xsumを算出
203
受信した乱数で
サム値Xsumを暗号化
204
データ送信処理
205
終了

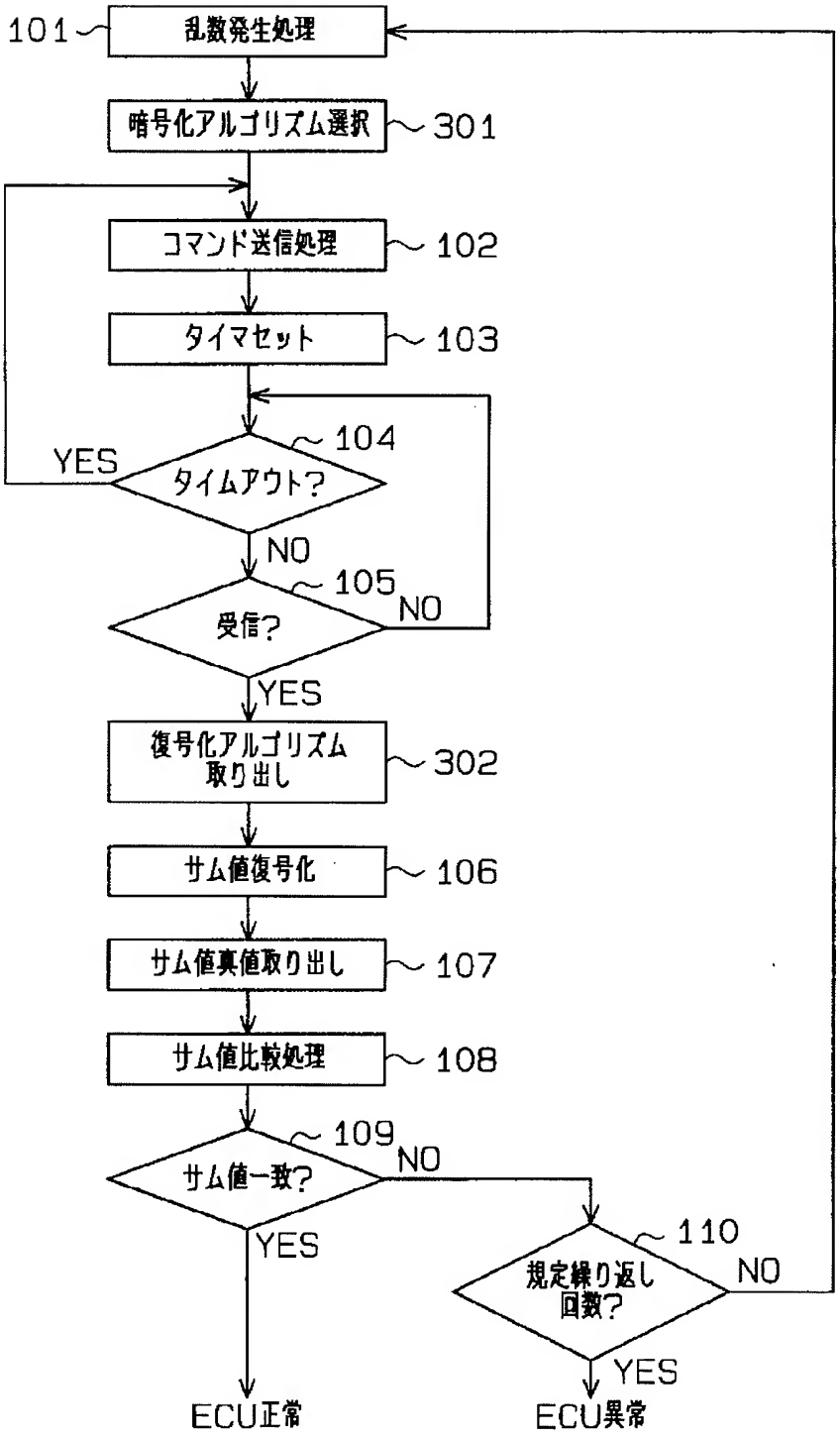
【図６】


ECU
10
(2) サム値Xsumを算出
(3) 算出式取り出し
(4) 暗号化
Xt=f (Xsum, Rt)
外部ツール
20
(6) 算出式取り出し
(7) 復号化
Xsum=f⁻¹ (Xt, Rt)
(8) サム値を比較判定
(5) Xt (乱数、算出式により決定)
L1
(1) サム値算出指令
+Rt
+ID
ID
算出式
0x01
f (*, *)
0x02
g (*, *)
0x0F
t (*, *)

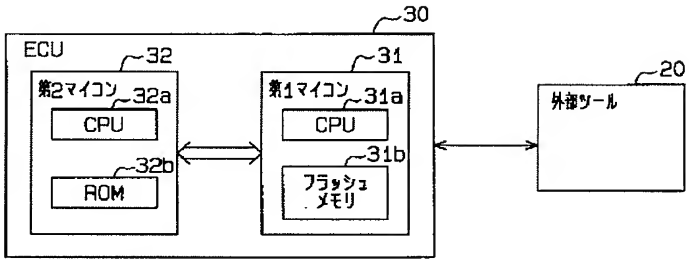
【図８】


NO
401
コマンド受信?
YES
受信データから乱数Rtと
アルゴリズムNo.抽出
402
サム値Xsumを算出
403
指定の暗号化アルゴリズム
取り出し
404
サム値Xsumを暗号化
405
データ送信処理
406
終了

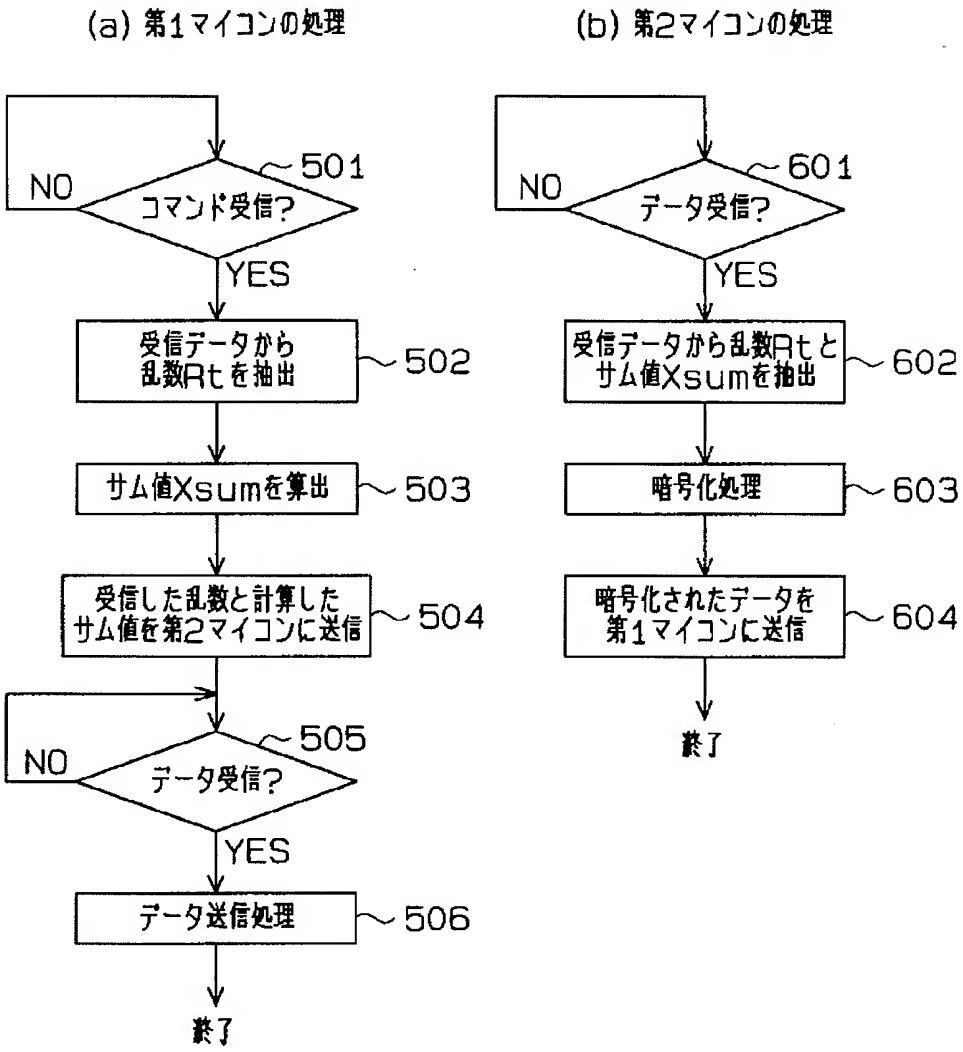
【図７】


101
乱数発生処理
暗号化アルゴリズム選択
301
コマンド送信処理
102
タイマセット
103
104
YES
タイムアウト?
NO
105
受信?
NO
YES
復号化アルゴリズム
取り出し
302
サム値復号化
106
サム値真値取り出し
107
サム値比較処理
108
109
サム値一致?
NO
YES
110
規定繰り返し
回数?
NO
YES
ECU正常
ECU異常

【図９】


30
ECU
32
第2マイコン
32a
CPU
32b
ROM
31
第1マイコン
31a
CPU
31b
フラッシュメモリ
20
外部ツール

【図１０】


(a) 第1マイコンの処理
NO
501
コマンド受信?
YES
受信データから乱数Rtを抽出
502
サム値Xsumを算出
503
受信した乱数と計算したサム値を第2マイコンに送信
504
NO
505
データ受信?
YES
データ送信処理
506
終了
(b) 第2マイコンの処理
NO
601
データ受信?
YES
受信データから乱数Rtとサム値Xsumを抽出
602
暗号化処理
603
暗号化されたデータを第1マイコンに送信
604
終了

フロントページの続き

(72)発明者　青木　千鶴
愛知県刈谷市昭和町１丁目１番地　株式会
社デンソー内

Ｆターム(参考)　5B048 AA14 CC02 DD06